

1 DANIEL L. WARSHAW (Bar No. 185365)
dwarshaw@pswplaw.com
2 PEARSON, SIMON, WARSHAW & PENNY, LLP
15165 Ventura Boulevard, Suite 400
3 Sherman Oaks, CA 91403
Telephone: (818) 788-8300
4 Facsimile: (818) 788-8104

5 JAMES J. PIZZIRUSSO (pro hac to be submitted)
jpizzirusso@hausfeldllp.com

6 HAUSFELD, LLP
1700 K Street NW
7 Washington, DC 20006
Telephone: (202) 540-7200
8 Facsimile: (202) 540-7201

9 [Additional counsel listed on signature pages]

10 Attorneys for Plaintiff Joshua Kairoff and All
Others Similarly Situated

11
12 UNITED STATES DISTRICT COURT
13 NORTHERN DISTRICT OF CALIFORNIA

14
15 JOSHUA KAIROFF, on Behalf of Himself
and All Others Similarly Situated,

16 Plaintiffs,

17 vs.

18 DROPBOX, INC., a Delaware corporation,

19 Defendant.
20
21
22
23
24
25
26
27
28

FILED
2011 MAY 23 P 3:24
RICHARD W. WIEKING
CLERK U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
(99) 155

E-filing

JCS

CV 11 2508

CASE NO.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

PEARSON, SIMON, WARSHAW & PENNY, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

1 Plaintiff Joshua Kairoff ("Plaintiff"), on behalf of himself and all others similarly situated,
2 alleges the following:

3 **I. INTRODUCTION**

4 1. Defendant Dropbox, Inc. ("Dropbox" or "Defendant") is a popular Internet based
5 file storage, synchronization, and sharing software program that allows users to store and access
6 their documents, media and other files on multiple devices. As with any data storage service, one
7 of the most important factors driving consumer decisions to subscribe to Dropbox is whether their
8 important personal and/or business information is maintained in the safest and most secure manner
9 possible.

10 2. In order to induce consumers to purchase and utilize Dropbox, Defendant has made
11 numerous false and misleading misrepresentations, including claims that user files are "always
12 safe," "inaccessible by third parties including Dropbox employees" and stored utilizing "the best
13 tools and engineering practices available." Contrary to these representations, Dropbox does not in
14 fact utilize the most secure methods available to protect its data from access to third parties, allows
15 employees to have access to user data, and has failed to take adequate measures to protect
16 sensitive financial, business and private user information from unauthorized access. Indeed,
17 during the class period and unbeknownst to users, Dropbox accessed purportedly encrypted and
18 secure customer data in order to eliminate duplicate files from being uploaded on its server and in
19 turn save money on bandwidth and storage costs.

20 3. Plaintiff Joshua Kairoff and other similarly situated class members relied on
21 Dropbox's representations regarding the safety and security of its software and would not have
22 paid as much for their Dropbox Pro subscription, if at all, but for Dropbox's false and misleading
23 representations regarding its safety and security. Plaintiff brings this action on behalf of a
24 nationwide class of all similarly situated individuals and entities who purchased a paid Dropbox
25 Pro subscription.

26 4. Through this lawsuit, Plaintiff is seeking injunctive relief prohibiting Dropbox from
27 continuing to engage in its false and misleading misrepresentations regarding the safety and
28 security of its product, as well as restitutionary relief and damages of all money paid by Plaintiff

1 and similarly situated class members for Dropbox Pro subscriptions.

2 **II. PARTIES**

3 5. Plaintiff Joshua Kairoff is an individual residing in Los Angeles County,
4 California. On or about September 26, 2010 Mr. Kairoff purchased an annual "Dropbox premium
5 service – 50 GB + 'Packrat' unlimited undo history" subscription for a price of \$138.00. Mr.
6 Kairoff has utilized Dropbox to store important personal, business and financial information. In
7 choosing to subscribe to Dropbox, Mr. Kairoff reviewed and relied on Defendant's representations
8 regarding the safety and security of its service, including representations that third parties, as well
9 as Defendant's employees, would not have access to user information; and that Dropbox utilized
10 the industry's top security measures to protect the confidentiality of user information. Plaintiff
11 would not have subscribed to Dropbox or paid as much for his Dropbox subscription but for
12 Defendant's false and misleading representations.

13 6. Defendant Dropbox, Inc. is a Delaware corporation with its principal place of
14 business and corporate headquarters located at 760 Market Street, Suite 1150, San Francisco, CA
15 94102. At all relevant times alleged herein, Dropbox made its business and marketing decisions
16 from its corporate headquarters in San Francisco, California.

17 **III. JURISDICTION AND VENUE**

18 7. This Court has jurisdiction over the subject matter presented by this Complaint
19 because it is a class action arising under the Class Action Fairness Act of 2005 ("CAFA"), Pub. L.
20 No. 109-2, 119 Stat. 4 (2005), which explicitly provides for the original jurisdiction of the Federal
21 Courts over any class action in which any member of the Plaintiff Class is a citizen of a state
22 different from any Defendant, and in which the matter in controversy exceeds in the aggregate the
23 sum of \$5,000,000.00, exclusive of interest and costs.

24 8. Plaintiff alleges that the total claims of the individual members of the Plaintiff
25 Class in this action are in excess of \$5,000,000.00 in the aggregate, exclusive of interest and costs,
26 as required by 28 U.S.C. § 1332 (d)(2).

27 9. As set forth above, Plaintiff is a citizen of California, and Defendant can be
28 considered a citizen of either California or Delaware. Therefore, diversity of citizenship exists

1 under CAFA, as required by 28 U.S.C. § 1332 (d)(2)(A).

2 10. Furthermore, Plaintiff alleges on information and belief that more than two-thirds
3 of all of the members of the proposed Plaintiff Class in the aggregate are citizens of a state other
4 than California where this action is originally being filed, and that the total number of members of
5 the proposed Plaintiff Class is greater than 100, pursuant to 28 U.S.C. § 1332(d)(5)(B).

6 11. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391(a) and (c)
7 because Defendant Dropbox resides in the district and a substantial part of the events or omissions
8 giving rise to the claims occurred in this district and the parties have contracted to adjudicate their
9 disputes in this district.

10 12. The Declaration of Daniel L. Warshaw, Pursuant to California Civil Code §
11 1780(c) regarding venue under the California Consumers Legal Remedies Act, Civil Code §§
12 1750 *et seq.* is attached hereto as Exhibit "A."

13 **IV. CHOICE OF LAW**

14 13. California law governs the claims asserted herein by Plaintiff and the Class
15 Members.

16 14. Each Dropbox user and member of the Class is subject to a choice of law provision
17 in the Dropbox Terms of Services which provides in relevant part as follows:

18 **Controlling Law and Jurisdiction**

19 These Terms of Service and any action related thereto will be
20 governed by the laws of the State of California without regard to its
21 conflict of law provisions. The exclusive jurisdiction and venue of
22 any action with respect to the subject matter of these Terms of
23 Service will be the state and federal courts located in San Francisco
24 County, California, and each of the parties hereto waives any
25 objection to jurisdiction and venue in such courts.

26 15. Additionally, upon information and belief, Dropbox's acts and omissions discussed
27 herein were orchestrated and implemented at Dropbox's headquarters in San Francisco, California.

28 16. California, which seeks to protect the rights and interests of California and other
U.S. residents against a company doing business in California, has a greater interest in the claims
of Plaintiffs and the Class Members than any other State.

17. Application of California law with respect to the claims of Plaintiff and the Class

Members is neither arbitrary nor fundamentally unfair because California has significant contacts to the claims alleged herein and a significant aggregation of contacts that create a state interest.

V. FACTUAL ALLEGATIONS

A. **Background on Dropbox File Sharing, Storage and Synchronization Services**

18. Dropbox provides a software program that allows consumers to synchronize and store their documents, videos and other electronic files on multiple devices and access them from any computer via "the cloud."

19. The principle behind "cloud computing" is that any computer connected to the Internet can be connected to the same pool of applications and files. Users can store and access files over the Internet rather than physically carrying around a storage medium such as a DVD or USB thumb drive.

20. Once a user downloads the Dropbox software, Dropbox creates a folder onto the user's computer. When a user puts a file into that folder, it is automatically saved on Dropbox's servers and purportedly secure.

21. Moreover, unlike saving files onto a single computer hard drive, saving files on a Dropbox folder will automatically save the file to all of a customer's Dropbox installed devices as well the Dropbox website. Accordingly, Dropbox allows user files to be simultaneously saved and synchronized among multiple computing devices (e.g. a work computer, home computer, iPad, Smartphone) and accessible from anywhere via the Internet utilizing the Dropbox website.

22. According to Defendant's promotional materials, the benefits and features of their service are described as follows:

Dropbox makes all your files available to you from any computer or phone. It's as easy as adding any file to your Dropbox folder. You can start working at the office and finish from home without ever needing to think about where your files are -- they are always with you.

Joining Dropbox is easy: installing the Dropbox software (free for Windows, Mac and Linux) creates a special folder on your computer. Anything you add to this Dropbox folder will automatically save to all your computers and to the Dropbox website. You can also invite people to share any folder in your Dropbox. This makes Dropbox perfect for team projects or sharing photos with family or friends -- it will be as if you are saving

straight to their desktop. The Dropbox mobile apps (free for iPhone, Android and Blackberry) let you take your life on the road. And because Dropbox keeps a one month history of your work, you can go back in time to fix mistakes or rescue deleted files.

23. By allowing files to be synchronized, stored and accessed from multiple computer devices, Dropbox provides certain features to consumers that are not available utilizing traditional hard drive data storage. First, saving files by utilizing Dropbox allows for automatic data synchronization so that users do not have to manually save files on multiple devices. Second, Dropbox can be utilized to back-up files to ensure they will not be destroyed in the event that a computing device is lost or destroyed. Third, Dropbox allows users to share their files with other people by utilizing "share folders" as an alternative to e-mail attachments or sending disks and flash drives.

24. Dropbox's subscription services are offered through tiered pricing that is predicated on the amount of storage capacity available to the user. Dropbox provides 2 gigabytes ("GB") of storage space to its customers for free. Consumers can purchase additional storage space, by signing up for one of two "Dropbox Pro" service plans, offering 50 GB of storage for \$9.99/month or \$99/year ("Pro 50"), and 100 GB of storage for \$19.99/month or \$199/year ("Pro 100").

25. Since its inception in 2007, Dropbox has been growing exponentially and is currently considered one of the hottest internet startup companies in the United States. Dropbox claims that it currently has 25 million registered users who save 200 million files a day on Dropbox. Dropbox's yearly revenue in 2011 from its data storage services has been projected by various sources to be \$100 million. Thus, it is estimated that approximately 750,000 to 1,000,000 users have paid for a Dropbox Pro subscription.

B. Dropbox Made Numerous False and Misleading Representations Regarding the Safety and Security of User Data

26. As with any file storage services provider, one of the key concerns for consumers is whether their important personal, private and financial data will be safely and securely stored in order to ensure that it is inaccessible by third parties, including Dropbox employees and agents. Recognizing this fact, until very recently, Dropbox prominently featured the purported safety,

1 security and inaccessibility of files stored on Dropbox. These purported safety and security
 2 measures served as the key selling points for Dropbox and were intended to convince consumers
 3 that the information they stored via Dropbox would be protected from disclosure and unauthorized
 4 access by anyone, including Defendant's employees and agents.

5 27. One of the four key points highlighted on the Dropbox install page that is viewed
 6 by consumers who download Dropbox states "Your files are always safe."

7 28. Similarly, the key features highlighted on the Dropbox fact sheet emphasize the
 8 safety and security of the product including the inability of Dropbox employees to view a user's
 9 files. Specifically, the drop box fact sheet states that:

10 *Your stuff is safe*

11 *Dropbox protects your files without you needing to think about it.*

- 12 • Dropbox keeps a one-month history of your work.
- 13 • Any changes can be undone, and files can be undeleted.
- 14 • *All transmission of file data occurs over an encrypted channel*
 15 *(SSL) and all files stored on Dropbox are encrypted.*
- 16 • *Dropbox employees are unable to view user files.*

17 (Emphasis added.)

18 29. A page in the help section of Dropbox's website entitled "How secure is
 19 Dropbox?" further boasts about the safety and security measures taken by the company. Plaintiff
 20 is informed and thereon alleges that prior to April 14, 2011 this help page contained the following
 21 representations regarding Dropbox's security measures.

22 Your files are actually safer while stored in your Dropbox than on
 23 your computer in some cases. We use the same secure methods as
 banks and the military.

24 Dropbox takes the security of your files and of our software very
 25 seriously. We use the best tools and engineering practices available
 26 to build our software, and we have smart people making sure that
 Dropbox remains secure. Your files are backed-up, stored securely,
 and password-protected...

27 All transmission of file data occurs over an encrypted channel
 28 (SSL).

1 All files stored on Dropbox servers are encrypted (AES-256) and are
2 inaccessible without your account password.

3 Public files are only viewable by people who have a link to the
4 file(s). Public folders are not browsable or searchable.

5 **Dropbox employees aren't able to access user files, and when
6 troubleshooting an account they only have access to file
7 metadata (filenames, file sizes, etc.) not the file contents.**

8 (Emphasis added.)

9 30. The principle and purpose behind these representations is to ensure consumers that
10 they can feel safe utilizing Dropbox because it utilizes the best and most secure data protection
11 practices available on the market and their personal information will not be accessible to anyone,
12 including Dropbox employees. By touting the safety and security of Dropbox as a key selling
13 point, Defendant has recognized and admitted the importance of these security features on
14 consumer decisions to use and purchase Dropbox.

15 **C. Dropbox's Representations Regarding the Safety and Security of Its Data are
16 False and Misleading**

17 31. The safety, security and accessibility of information stored by Dropbox is dictated
18 by the data encryption protocols utilized by the company. Data encryption refers to the process of
19 transforming electronic information into a scrambled code that can only be read by someone who
20 knows the key or password necessary to remove the code. Utilizing proper data encryption
21 methods allows individuals to securely transmit data over unsecured internet connections, such as
22 in public wireless networks in coffee shops and store data in a manner that does not allow third
23 parties to access the underlying information, even in the event that the data or device is lost or
24 stolen.

25 32. Unlike a consumer purchase transaction in which the customers intend for a
26 company to access their information, the purpose of the Dropbox service is for no one (unless
27 dictated by the user), including Defendant and its employees, to have access to the private
28 information stored on Dropbox. Indeed, allowing this type of access to user information
essentially defeats the purpose behind subscribing to a purportedly secure system like Dropbox.

33. In order to assure consumers that their data is secure, Dropbox repeatedly

1 represented during the class period that any data stored on its system utilized the most secure
2 encryption methods available and was not accessible to anyone *including* Dropbox employees.

3 34. Contrary to Dropbox's express representations, however, the information stored
4 using the Dropbox service is stored utilizing encryption keys known to Dropbox, through which
5 its employees are able to access users' data without their knowledge or consent. Dropbox claims
6 it is against the company's policy for most employees to access this data, but this is far different
7 from employees having *no* access to the data at all as Dropbox misrepresented.

8 35. Furthermore, Dropbox's use and storage of encryption keys does not follow the
9 "best practices" for the "cloud" storage industry. Indeed, several competing services, such as
10 SpiderOak and Wuala, encrypt user data utilizing a key only known to the respective customer,
11 which prevents even their own employees and agents from accessing or stealing the unprotected
12 data stored on their servers. In fact SpiderOak states:

13 [W]e at SpiderOak decided to never store a user's password nor the
14 plaintext of a user's encryption keys. This ensures that there can
15 never be a point - ever - where we could even unknowingly betray
16 the trust or privacy of a user. Why? Because - to put it simply - we
17 don't ever come into contact with the keys needed to unlock the
18 encryption surrounding the data. Even with physical access to the
19 server or under subpoena, SpiderOak simply can never see or turn
20 over a user's plaintext files, filenames, file sizes, file types, etc... On
21 the server, we only see sequentially numbered containers of
22 encrypted data.¹

23 36. One of the reasons that Dropbox has chosen a product design in which the
24 company and its employees have access to user data is that doing so enables the company to save
25 money. This design enables Dropbox's software to automatically scan, access, and detect
26 duplicate files stored by multiple users (e.g. duplicate Mp3 files, videos, documents etc.). This
27 means that if two or more users attempt to store the exact same file in their respective Dropbox
28 accounts, Dropbox will only actually upload and store a single copy of the file on its server
thereby saving bandwidth and storage costs and gaining a competitive advantage over other

¹ <http://spideroak.com/blog/200811201300> (Last viewed on May 20, 2011).

1 similar companies who do not access user files and do not eliminate duplicate files across different
 2 accounts. By coupling the financial advantages associated with Dropbox's system design and its
 3 access to users' unencrypted data, with the aforementioned statements denying that such access
 4 exists, Dropbox is able to offer a product that is significantly less secure than its competitors but at
 5 a premium price, thereby fraudulently inducing its users and gaining a strategic competitive
 6 advantage over other data storage providers.²

7 37. Dropbox has also misrepresented the safety and security of information transmitted
 8 on mobile devices by claiming that, "All transmission of file data occurs over an encrypted
 9 channel (SSL)." In truth, Dropbox does not use SSL to transmit "metadata" (such as the names of
 10 files), via the Dropbox mobile client, which is used by customers on their phones and other mobile
 11 devices. As a consequence, malicious persons using the same wireless network as a Dropbox
 12 mobile user can observe the metadata associated with a user's files as they are transmitted between
 13 the user's mobile device and Dropbox's server. This can reveal, for example, the names of
 14 confidential files and documents, which could themselves be highly sensitive (for example,
 15 resignation-letter.doc, or information-about-breast-cancer.doc). The mobile versions of competing
 16 cloud services, such as SpiderOak, do not suffer from this same design flaw, and encrypt all data,
 17 both the metadata, and the contents of files, both in storage, and in transit. Without knowledge of
 18 this important fact, consumers are more likely to subscribe to Dropbox and utilize Dropbox's
 19 mobile services in order to transmit sensitive and private information via their mobile devices.

20 38. Therefore, Dropbox has made material misrepresentations to consumers because, in
 21 contrast to direct statements it made in advertising and promotional materials, it has, *inter alia*: (1)
 22 failed to take adequate steps to secure and encrypt data to prevent access by third parties including
 23

24 ² Dropbox currently charges more for its data storage services than both SpiderOak and Wuala.
 25 SpiderOak offers 100 GB of data storage for \$10/month or \$100 per year, which is the
 26 approximate price that Dropbox charges for 50 GB of data storage. See
 27 <https://spideroak.com/pricing> (last viewed on May 16, 2011). Wuala offers 100 GB of data
 28 storage for \$129 per year which is also significantly cheaper than Dropbox. See
<http://www.wuala.com/en/pricing> (last viewed on May 16, 2011).

Defendant's employees and agents; (2) failed to employ the most restrictive industry security measures that are utilized by its competitors; (3) accessed user information without consent; and (4) failed to ensure that all data transmitted via mobile phone devices occurs over an encrypted channel.

D. Revelation that Dropbox Has the Ability to View User Data Causes Outrage Among Dropbox Users and the Tech Community

39. In April of 2011, the fact that Dropbox has access to user data in direct contravention to its previous representations was publicly disclosed by a privacy advocate. On April 12, 2011, Christopher Soghoian, a Graduate Fellow at the Center for Applied Cybersecurity Research, and a Ph.D. Candidate in the School of Informatics and Computing at Indiana University, published an article entitled "How Dropbox Sacrifices User Privacy for Cost Savings." Mr. Soghoian's article disclosed that contrary to Dropbox's representations regarding user safety and security, Dropbox has been accessing and deduplicating user data in order to save bandwidth and storage space.

40. After the public disclosure of Dropbox's misrepresentations regarding its security and privacy policies, a number of users and technology commentators complained regarding Dropbox's policies and their misrepresentations.

41. Comments left on Dropbox's support forums³ and Dropbox's founders' blog postings⁴ make it clear that many Dropbox customers were extremely upset that the company had "lied" to them. A sampling of these complaints is set forth as follows (misspellings and typographical errors in original):

DT:

This is just terrible, so YOU are able to access our data but "not" allowed too, that's fine, but it means that you have our keys to decrypt our files, no? Take a look at what happened to SONY PSN, what if someone hacks into Dropbox, takes all our keys, decrypt things at their will or put the DB on PirateBay, or.....?

³ <http://forums.dropbox.com/topic.php?page=2&id=36814> (Last viewed on May 17, 2011).

⁴ <http://blog.dropbox.com/?p=735> (Last viewed on May 17, 2011).

1 This questions a lot of things, if you are able to decrypt all the data
2 without our passwords it means that any one can.

3 I'm really disappointed, i Loved soooo much Dropbox :(

4 **Ewan Leith:**

5 I don't feel like we were misled, I know we were misled, let's be
6 clear on it.

7 Previously your help page said:

8 "Dropbox employees aren't able to access user files, and when
9 troubleshooting an account they only have access to file metadata
10 (filenames, file sizes, etc., not the file contents)"

11 The full page is still in Google Cache at
12 <http://webcache.googleusercontent...>

13 We now know this isn't true. It's not "misleading", it's a straight-
14 forward lie. Dropbox employees are able to access user files, but
15 you have policies and technical solutions in place to control their
16 access. It's a fundamental distinction.

17 **Guest:**

18 Two things:

19 1. I've used the service thinking that Dropbox employees are NOT
20 ABLE to access my data.

21 2. Now, I know that they, in fact, have no issues accessing it.

22 Now my question: Should I trust them that if I cancel my
23 subscription completely and ask them to delete data, they will
24 comply? And will not make a backup somewhere for "future
25 reference" or whatever other purposes they may have?

26 **Chase Parker:**

27 I'm sorry, this excuse simply doesn't wash. You didn't say
28 "Dropbox employees aren't ALLOWED to access user files", you
said "Dropbox employees aren't ABLE to access user files". No
amount of prevarication on your part will convince me that your
intent with the old wording wasn't to convey the notion that access
to encrypted customer data wasn't possible. It won't convince me
because that was CLEARLY your intent, and anyone reading the old
wording can see that for themselves.

. . . And I'm sorry, but your responses to this concern seem not to
come from an honest desire to restore our trust in you, but seem
designed to minimize any legal liability you had for quite clearly
and explicitly misleading your customers in both your TOS and your
website.

1 It is this issue, and no other, that makes it impossible for me to trust
 2 your company or your service at the moment. If you had just copped
 3 to it and admitted that your old wording was flat-out deceptive and
 4 explained WHY it happened that way, I would have been amenable
 to further explanation. But the fact that you're STILL trying to
 pretend that it was a poor choice of wording instead of manifest and
 blatant misinformation makes that impossible.

5 I'm sorry, this just isn't something you can "make right" any longer.
 6 You had your chance to do so, and you used that chance to dodge
 7 and weave instead. I can no longer recommend that users trust your
 8 service when it comes to data security due to the simple fact that you
 have proven yourselves willing to deliberately mislead your
 customers when it suits your legal interests.

9 It really is a shame.

10 **Raphael:**

11 I am from the people that subscribed BECAUSE of the promise they
 12 put forward at the time of encrypted file content encrypted with the
 user password that even DropBox employees could not access.

13 Also, worth of note, DropBox installs notification software on the
 14 Mac without even mentioning it (Growl) even less asking the user.

15 For me, that's two breach of trust in a row. It cannot be an accident.
 At DropBox, there seem to be a disconnect between what they
 pretend to care about and what they really care about.

16 **Christopher Parker:**

17 It seems pretty clear to me... I've CAPITALIZED the parts that spell
 18 this out:

19 "Dropbox employees AREN'T ABLE TO ACCESS USER FILES,
 20 and when troubleshooting an account they ONLY HAVE ACCESS
 TO FILE METADATA (filenames, file sizes, etc., NOT THE FILE
 CONTENTS)."

21 Notice how there are no exceptions noted here. No caveats. Nothing
 22 to lead a reasonable person to believe there are any circumstances
 that would go against this statement.

23 This statement, coupled with the statement that everything was
 24 encrypted with "military-grade AES256 encryption", told users that
 25 it was NOT POSSIBLE to decrypt the contents of users' files. Any
 reasonable person would infer that this meant there was no way for
 anyone to access file contents, since they weren't ABLE TO do so.

26 ...

27 It's really not an assumption if all of the parts were there, just as it
 28 isn't an assumption to infer that a person has four limbs if they only
 tell us they have exactly two arms and exactly two legs.

Raphael:

I second that! And in other part of the documentation they insisted at the time that nothing could be done to recover the data if the password was lost.

I signed on the belief that the key way my password. Why? Because that make sense: a user password does not need to be stored anywhere, making it REALLY impossible for any employee to decrypt the content of a file.

I believe now that this was the original intent of the DropBox founders. Later on, when they realized the difficulty of maintaining the system, the dropped it without telling anyone. But they kept the now misleading wording. This is just plain dishonest.

Xanathon:

Main Problem is that you tried to change the TOS behind our backs without informing your users openly and transparently. My files are now in a TrueCrypt-Container but I will definitely look for an alternative to Dropbox and will use that as soon as possible.

Justin Cardinal:

FWIW, I considered creating a TrueCrypt volume to store sensitive data within my Dropbox account. After reading their information that said the information was encrypted and that their own employees couldn't access it, I made a conscious decision that the extra layer was unnecessary because the data was already secure. That's the problem; people made decisions about the security of their data based on what Dropbox claimed, and now it turns out those claims were untrue.

Guest:

To everyone who's saying that we should have known better, you're completely missing the point, which is that Dropbox told us one thing and is now telling us another. They LIED when they said even their employees couldn't access the data. See Ewan Leith's post.

Who's to say they're not lying now? What's preventing a rogue employee from searching through files for interesting tidbits? Nothing.

They're purposely misleading the media by changing the argument. It's shady, and I'll be taking my files elsewhere.

Xyzzzy:

DropBox could store everything in an encrypted format, and without storing the decryption keys. That way nobodoy -- NOBODY -- could decrypt that data without my password. As furstbox notes above, Wuala does exactly this.

1 <http://www.wuala.com/en/learn/...>

2 As Drew and Arash explain above, they made a conscious decision
3 to do things differently. They instead encrypt data, but store the
4 encryption/decryption keys at the DropBox servers. They did so
5 because they it allows DropBox to have additional features.

6 That's a reasonable position. I'm not upset about DropBox using
7 this method of security -- it might be good enough for most people,
8 and provide for better features. However, I am upset about them
9 misleading us with their prior statements that nobody at DropBox
10 has the ability to decrypt my data. That was a lie.

11 **Ian Buchanan:**

12 I am sad that Dropbox has access to our files. I have convinced my
13 company that we can use this service for our project files, instead of
14 using a VPN into our companies servers. They were sold on the fact
15 that the files are encrypted. I expect that we will have to stop using
16 this service, to which we buy about 40-50 50GB licenses each year.

17 I am wondering if any of you guys know how the Wuala.com guys
18 are accomplishing what Dropbox says is impossible. Are they lying
19 too?

20 **Roy Sablosky:**

21 This is an endearing letter, but I just cannot overlook the difference
22 between "we CANNOT decrypt your files" and "we WILL NOT
23 decrypt your files unless the FBI asks us to." Those statements are
24 not the same. Maybe it's technically challenging -- even impossible
25 -- to provide the level of security promised in the original TOS. The
26 fact remains that you did promise it. You haven't changed the
27 service, you've only removed the misleading language from your
28 TOS. Apparently you can and will hand over my stuff to the feds if
they ask nicely. There are other services that CANNOT hand over
my data even if the police threaten them with violence. That's what
you promised and that's how it ought to be. So, even though I
personally have nothing to hide, I am terminating my relationship
with Dropbox.

21 **Lizzy:**

22 Dropbox, how do we know if you've stolen our proprietary business
23 trade secrets or not? Our company can no longer trust you

24 **Kevin Barbee:**

25 I feel you need to do something for existing users. Basically, your
26 marketing materials lied saying no one had access if you lost your
password, when obviously that isn't true.

27 Step up to the plate, admit you didn't reveal everything. Give
28 people a free month.

Or, face class action suits claiming fraud.

Step up.

Zugu:

That's it, I'm done with Dropbox. I hope the FTC drops a heavy fine on you and that you lose a lot of your customers, because you LIED.

Me M:

The problem is, I could have sworn that some Dropbox employee stated on these forums that even Dropbox themselves couldn't decrypt your files...

Matthew P:

I agree with "Me. M." - I was told that Dropbox employees couldn't decrypt files even if they wanted to. Now I'm wondering how many rogue employees have copies of my financial information.

Dima P.:

Good, won't be using Dropbox for any business or sensitive data. Will advise my friends and colleges the same.

42. The sentiments of Dropbox users have been echoed by technology reporters and professionals who have expressed their concerns that they were deceived by Dropbox's representations.

43. For example, on April 19, 2011, Jon Callas, a professional cryptographer and co-founder and former C.T.O. of Pretty Good Privacy posted on his public Twitter account: "I deleted my Dropbox account. It turns out that they lied and don't actually encrypt your files and will hand them over to anyone who asks."

44. Richard Gaywood at the Unofficial Apple Weblog commented that, "Dropbox's FAQ copy makes it sound like its employees don't have access to [the user encryption] key - - as though it's generated from your Dropbox password, perhaps. That's certainly what I took away from the Dropbox FAQ."

45. In an article entitled, "Dropbox Drops the Ball on Data Security," PCWorld.com wrote:

At issue are Dropbox's terms of service. Previously, the company stated in its terms of service that 'all files stored on Dropbox servers are encrypted (AES-256) and are inaccessible without your account

password.' But, Dropbox has continued to modify the terms of service, and backpedal on exactly how secure customer data is--sometimes putting its foot in its proverbial mouth. ***Dropbox has been at least confusing, if not misleading, about just how secure data really is.*** After a few amendments, the terms have been altered such that it now reads more to the effect that Dropbox can access and view your encrypted data, and it might do so to share information with law enforcement if it is compelled, but that employees are prohibited from abusing that power and viewing customer data. According to encryption expert Vormetric, the root of the Dropbox scenario is that the keys used to encrypt and decrypt files are in the hands of Dropbox, not stored on each user's machine. While Dropbox might have policies prohibiting Dropbox employees from viewing files, a rogue employee could view customer data using the keys held by Dropbox.

(emphasis added)

46. Rather than taking concerted action to improve and revise its security measures to conform to its express representations, Dropbox has responded by making modifications to its Terms of Service and representations regarding its security measures and changing its policies -- all without adequately informing its paying customers. Importantly, Dropbox has not sent out a general notice to all users to let them know of these changes and has only modified language on parts of its website, while some of its key misrepresentations (including that employees cannot access files) remain available on other parts of the site, such as its "Fact Sheet."

47. Further, Dropbox has not offered refunds or any compensation to the hundreds of thousands of users who relied on its previous misrepresentations and are stuck in monthly or year-long contracts that Dropbox claims are non-refundable. Dropbox's terms state:

Dropbox Premium Accounts are prepaid and are non-refundable. DROPBOX DOES NOT PROVIDE REFUNDS OR CREDITS FOR ANY PARTIAL MONTHS OR YEARS. You may cancel your Dropbox Premium Account at anytime, and cancellation will be effective immediately. If you wish to cancel your Premium Account you may do so via your 'Account' page. Should you elect to cancel your Premium Account, please note that you will not be issued a refund for the most recently (or any previously) charged monthly fees.

48. Dropbox has now modified and revised its "How Secure is Dropbox" page as follows:

a. Dropbox has deleted its statement that: "Online access to your files requires your username and password."

b. The statement "Nobody can see your private files in Dropbox unless you deliberately invite them or put them in your Public folder" was modified to be "Other Dropbox users can't see your private files in Dropbox unless you deliberately invite them or put them in your Public folder."

c. Dropbox has deleted the representation that: "Dropbox employees aren't able to access user files, and when troubleshooting an account they only have access to file metadata (filenames, file sizes, etc, not the file contents)."

d. Dropbox has also added the following language to its website:

Dropbox employees are prohibited from viewing the content of files you store in your Dropbox account, and are only permitted to view file metadata (e.g., file names and locations). Like most online services, we have a small number of employees who must be able to access user data for the reasons stated in our privacy policy (e.g., when legally required to do so). But that's the rare exception, not the rule. We have strict policy and technical access controls that prohibit employee access except in these rare circumstances. In addition, we employ a number of physical and electronic security measures to protect user information from unauthorized access.

49. Dropbox has also made changes to its Terms of Service to disclose further information regarding its policies and protocols for sharing user information with law enforcement, in order to ostensibly "be more user friendly and more transparent." Ironically, in discussing these changes on a blog post, Dropbox's founders claimed that its old Terms of Service actually gave Dropbox more rights than it needed: "You'll notice that the new Terms of Service (TOS) better outlines the specific situations under which we would disclose user data. We felt our old TOS language was too broad, and gave Dropbox rights that we didn't even want."

50. Dropbox's belated actions are wholly insufficient, particularly to the extent that Dropbox continues to makes material misrepresentations regarding the extent of its security measures on its website and elsewhere and allows employee access to user data as set forth herein. As demonstrated by recent insider security breaches at Google, Facebook and the State Department and numerous breaches by hackers that targeted Sony, Epsilon and RSA, similar potential breaches here present a real danger to consumers and are a legitimate cause for concern. Unlike financial institutions and merchants who need to decode user data and do so with the

1 explicit consent of consumers, Dropbox has no legitimate need to access user data and cannot
2 justify permitting employees to access users' sensitive business and financial information.

3 51. Given the fact that class members utilize Dropbox to store their important and
4 valuable financial, personal and business information (such as attorney client privileged materials
5 and sensitive work product), the safeguarding of client information is of utmost importance to
6 consumers.

7 52. This change in Dropbox's language is also highly unlikely to be viewed by the
8 millions of Dropbox users who had signed up prior to April of 2011 and who were led to believe
9 and relied on Dropbox's assurance that their data was inaccessible by Dropbox and its employees.
10 Dropbox has not emailed its millions of users, for example, to inform them of these material
11 changes. Nor has Dropbox offered refunds to those who signed up for its services based on these
12 explicit representations. Given the fact that these current users already store their valuable
13 information on Dropbox, it is extremely difficult and burdensome for them to discontinue using
14 Dropbox even if such disclosures exist.

15 **E. Dropbox's False and Misleading Statements Have Caused Cognizable Injuries**
16 **to Plaintiff and Similarly Situated Class Members**

17 53. Dropbox's misrepresentations regarding the safety and security of its data storage
18 services were designed to induce reliance and were likely to and did deceive consumers including
19 Plaintiff and Class members to subscribe to induce Dropbox subscriptions. As a direct and
20 proximate result of Dropbox's false and misleading statements, reasonable consumers were led to
21 believe that their materials stored on Dropbox were transmitted and stored in a safe, secure, and
22 inaccessible manner utilizing the best and most secure industry practices available when they in
23 fact were not.

24 54. Plaintiff and the Class suffered injury in fact and have lost money as a result of
25 Dropbox's misconduct by subscribing to Dropbox Pro. Plaintiff and the Class would not have
26 purchased or paid as much for Dropbox Pro, but for the Defendant's misrepresentations regarding
27 the safety and security measures it purportedly took to protect customer data from unauthorized
28 access.

55. As a result of the misleading representations detailed above, Dropbox was able to charge a premium price and increase sales for its data storage and synchronization services over competing companies, many of whom do actually do what Dropbox falsely claimed to be doing: encrypt and protect user data. Defendant has reaped substantial profit and has been unjustly enriched by its misrepresentations of material fact regarding Dropbox, as set forth herein.

VI. RULE 9(b) ALLEGATIONS

56. WHO: Defendant Dropbox made material misrepresentations and failed to disclose, or adequately disclose, material facts as detailed herein. Except as identified herein Plaintiff is unaware, and therefore unable to identify, the true names and identities of those individuals at Dropbox who are responsible for such material misrepresentations and omissions.

57. WHAT: Defendant made material representations regarding the safety, security and confidentiality features of Dropbox. Specifically, Defendant represented to the Plaintiff and similarly situated class members that: (1) third parties, including Defendant's employees, would not have access to data stored by users utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive security measures to protect the confidentiality of user information; (3) Dropbox did not access user data; and (4) all transmission of file data occurs over an encrypted channel (SSL). Each of these representations were false and misleading because, Dropbox: (1) failed to take adequate steps to secure and encrypt data and the corresponding encryption keys to prevent access by third parties including Defendant's employees and agents; (2) failed to employ the most restrictive security measures such as those utilized by its competitors; (3) accessed user information without consent; and (4) failed to ensure that all user data transmitted via mobile phone devices occurs over an encrypted channel.

58. WHEN: Defendant made the affirmative material misrepresentation, omissions, and non-disclosures as detailed herein continuously from the inception of the company in June of 2007 and continues to do so through the present.

59. WHERE: Defendant's affirmative, material misrepresentations, omissions, and non-disclosures as detailed herein were made on the Internet (including on its website www.dropbox.com), in press releases and official company statements (such as Defendant's "Fact

Sheet”), in its terms of service and contractual materials, and other materials associated with the Dropbox software program.

60. HOW: Defendant made numerous, written material misrepresentations on its website promotional pages that were designed to and did in fact mislead Plaintiff and similarly situated class members to believe that Dropbox has security features and confidentiality provisions that it in fact did not. These material misrepresentations included statements that: (1) third parties including Defendant’s employees would not have access to data stored utilizing Dropbox; (2) Dropbox utilized the industry’s most restrictive security measures to protect the confidentiality of user information; (3) Dropbox did not access user’s files; and (4) all data transmitted via Dropbox was encrypted to ensure confidentiality.

61. WHY: Defendant engaged in the aforementioned affirmative material misrepresentations and omissions for the express purpose of inducing Plaintiff and similarly situated class members to utilize and subscribe to Dropbox’s paid service based on the belief that Dropbox has safety and security features that it in fact did not have. By allowing for the decryption of user information, Dropbox has been able to eliminate duplicate files thereby saving bandwidth and storage costs and gaining a competitive advantage over competitors who do not decrypt user files and do not eliminate duplicate files across different user accounts.

VII. CLASS ACTION ALLEGATIONS

62. Plaintiff brings this action on behalf of himself and all other similarly situated consumers as members of a proposed nationwide Class pursuant to Federal Rule of Civil Procedure 23.

63. The Class is defined as:

All individuals and entities residing in the United States who purchased a Dropbox Pro paid subscription. Excluded from the Class are Dropbox and its parent companies, subsidiaries, affiliates, officers and employees; any co-conspirators; all governmental entities; and any judges or justices assigned to hear any aspect of this action.

64. Plaintiff reserves the right to amend the class definition prior to class certification.

65. The Class is composed of an easily ascertainable, self-identifying set of individuals

1 and entities that purchased Dropbox Pro subscriptions. The Class can be readily identified
2 through Dropbox's records.

3 66. There is a well-defined community of interest among the proposed Class Members,
4 and the disposition of all of their claims in a single action will provide substantial benefits to all
5 parties and to the Court.

6 67. The claims of the representative Plaintiff are typical of the claims of the Class
7 Members in that the representative Plaintiff, like all Class Members, purchased a Dropbox Pro
8 subscription, which Dropbox advertised, promoted, marketed, warranted and sold as adequately
9 securing the information stored by consumers from unauthorized third party access.

10 68. The representative Plaintiff and all Class Members have been damaged by
11 Defendant's misconduct in that they did not get what they paid for.

12 69. The factual bases for Dropbox's misconduct are common to all Class Members and
13 represent a common thread of wrongdoing resulting in injury to all members of the Class.

14 70. Plaintiff will fairly and adequately protect the interests of the Class. He has
15 retained counsel with substantial experience in prosecuting consumer class actions, and
16 specifically actions involving defective products.

17 71. Plaintiff and his counsel are committed to prosecuting this action vigorously on
18 behalf of the Class, and have the financial resources to do so. Neither Plaintiff nor his counsel has
19 any interests adverse to those of the Class.

20 72. Plaintiff and the Class Members have all suffered and will continue to suffer harm
21 and damages as a result of Dropbox's unlawful and wrongful conduct.

22 73. The prosecution of separate actions by thousands of individual Class Members
23 would create a risk of inconsistent or varying adjudications with respect to individual Class
24 Members, thus establishing incompatible standards of conduct for Defendant.

25 74. The prosecution of separate actions by individual Class Members would also create
26 the risk of duplicative adjudications with respect to them that would, as a practical matter, be
27 dispositive of the interests of the other Class Members who are not a party to such adjudications
28 and would substantially impair or impede the ability of such non-party Class Members to protect

1 their interests.

2 75. Dropbox has acted or refused to act on grounds generally applicable to the entire
3 Class, thereby making appropriate final declaratory and injunctive relief with respect to the Class
4 as a whole.

5 76. There are numerous questions of law and fact common to Plaintiff and the Class
6 that predominate over any questions that may affect individual Class Members, and include the
7 following:

- 8 a. Whether Defendant made false and misleading statements regarding the
9 safety and security of its software which provides data storage and synchronization services;
- 10 b. Whether Defendant's conduct constitutes breach of express warranty;
- 11 c. Whether Defendant's conduct constitutes breach of the implied warranty of
12 fitness for a particular purpose;
- 13 d. Whether Defendant's conduct violated the California Consumers Legal
14 Remedies Act (Cal. Civ. Code §§ 1750, *et seq.*);
- 15 e. Whether Defendant's conduct violation California's unfair competition law
16 (Cal. Bus. & Prof. Code §§ 17200, *et seq.*);
- 17 f. Whether Defendant's conduct violated California's false advertising law
18 (Cal. Bus. & Prof. Code §§ 17500, *et seq.*);
- 19 g. Whether Plaintiff and the Class are entitled to compensatory, exemplary and
20 statutory damages, and the amount of such damages; and
- 21 h. Whether Dropbox should be ordered to disgorge, for the benefit of the
22 Class, all or part of the ill-gotten gains it received from the sale of Dropbox Pro, and/or to make
23 full restitution to Plaintiff and the Class Members.

24 77. Given: (i) the substantive complexity of this litigation; (ii) the size of individual
25 Class Members' claims; and (iii) the limited resources of the Class Members, few—if any—Class
26 Members could afford to seek legal redress individually for the wrongs Defendant has committed
27 against them.

28 78. Class treatment of common questions of law and fact would also be superior to

multiple individual actions or piecemeal litigation in that class treatment will foster an orderly and expeditious administration of Class claims, economies of time, effort and expense, and uniformity of decision.

79. This action presents no difficulty that would impede the Court's management of it as a class action, and a class action is the best and/or the only available means by which members of the Class can seek legal redress for the harm caused by Defendants.

80. Absent a class action, Class Members will continue to incur damages and Defendant's misconduct will continue without remedy.

81. A class action is superior to other available methods for the fair and efficient adjudication of the controversy.

82. The issues common to the claims of Plaintiffs and the Class Members, some of which are identified above, are alternatively certifiable pursuant to Fed. R. Civ. P. 23(c)(4), as resolution of these issues would materially advance the litigation, and class resolution of these issues is superior to repeated litigation of these issues in separate trials.

FIRST CAUSE OF ACTION

BREACH OF EXPRESS WARRANTY

83. Plaintiff and the Class incorporate by reference the allegations of the preceding paragraphs of this Complaint as if set forth in full herein.

84. Defendant is a merchant as defined by the applicable Uniform Commercial Code ("U.C.C.") provisions and sold services to Plaintiff and members of the Class.

85. Defendant is in direct privity with Plaintiffs and members of the Class by reason of its terms of service and the contractual relationship entered into between users and Dropbox when users downloaded the Dropbox software from Defendant's website.

86. Dropbox expressly warranted via its advertising, statements, brochures, website information, public statements, and disseminated information to the general public, including Plaintiff and the Class, *inter alia*: (1) third parties including Defendant's employees would not have access to data stored utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive

1 security measures to protect the confidentiality of user information; (3) Dropbox did not access
2 user data; and (4) all data transmitted via Dropbox was encrypted to ensure secure access.

3 87. The statements made by Defendant are affirmations of fact that became part of the
4 basis of the bargain and created an express warranty that its services would conform to the stated
5 promises. Plaintiff and Class members placed importance on Defendant's representations.

6 88. Defendant breached each of the aforementioned warranties and representations
7 because during the class period, Dropbox: (1) failed to take adequate steps to secure and encrypt
8 data to prevent access by third parties including Defendant's employees and agents; (2) failed to
9 employ the most restrictive security measures such as those utilized by its competitors; (3)
10 accessed user information without consent; and (4) failed to ensure that the data transmitted via
11 mobile phone devices occurred over an encrypted channel.

12 89. As a result of Dropbox's breach of the express warranty, Plaintiff and the Class
13 were injured in the amount of all or a portion of the purchase price of their Dropbox Pro
14 subscription.

15 **SECOND CAUSE OF ACTION**

16 **BREACH OF IMPLIED WARRANTY OF FITNESS FOR PARTICULAR PURPOSE**

17 90. Plaintiff and the Class incorporate by reference the allegations of the preceding
18 paragraphs of this Complaint as if set forth in full herein.

19 91. Defendant is a merchant as defined by the applicable U.C.C. provisions and sold
20 services to Plaintiff and members of the Class.

21 92. Defendant is in direct privity with Plaintiffs and members of the Class by reason of
22 its terms of service and the contractual relationship entered into between users and Dropbox when
23 users downloaded the Dropbox software from Defendant's website.

24 93. Defendant knew that Plaintiff and the Class intended to purchase Dropbox as a
25 means for securely storing their files and private information and were relying on Defendant's
26 technical skill and judgment in making their decision to purchase Dropbox.

27 94. Dropbox represented via its advertising, statements, website information, public
28 statements, and representations disseminated information to the general public, including Plaintiff

1 and the Class, that *inter alia*: (1) third parties including Defendant's employees would not have
 2 access to data stored utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive
 3 security measures to protect the confidentiality of user information; (3) Dropbox did not access
 4 user data; and (4) all data transmitted via Dropbox was encrypted to ensure secure access.

5 95. Defendant breached each of the aforementioned warranties and representations
 6 because during the class period, Dropbox: (1) failed to take adequate steps to secure and encrypt
 7 data to prevent access by third parties including Defendant's employees and agents; (2) failed to
 8 employ the most restrictive security measures such as those utilized by its competitors; (3)
 9 accessed user information without consent; and (4) failed to ensure that all user data transmitted
 10 via mobile phone devices occurred over an encrypted channel.

11 96. As a result of Dropbox's breach of implied warranty, Plaintiff and the Class were
 12 injured in the amount of all or a portion of their purchase price of their Dropbox Pro subscription.

13 **THIRD CAUSE OF ACTION**

14 **VIOLATION OF THE CALIFORNIA CONSUMERS LEGAL REMEDIES ACT**

15 (Cal. Civ. Code §§ 1750 *et seq.*)

16 97. Plaintiff and the Class incorporate by reference the allegations of the preceding
 17 paragraphs of this Complaint as if set forth in full herein.

18 98. Defendant has engaged in and continues to engage in business practices in violation
 19 of California Civil Code §§ 1750 *et seq.* (the "Consumers Legal Remedies Act") by making false
 20 and unsubstantiated representations concerning the characteristics of Dropbox. These business
 21 practices are misleading and/or likely to mislead consumers and should be enjoined.

22 99. Defendant has engaged in deceptive acts or practices intended to result in
 23 subscriptions to Dropbox in violation of California Civil Code § 1770. Defendant knew and/or
 24 should have known that its representations of fact concerning the characteristics, composition and
 25 quality of Dropbox's software were material and likely to mislead the public. Defendant
 26 affirmatively represented the safety and security features of Dropbox software including, *inter*
 27 *alia*: (1) third parties including Defendant's employees would not have access to data stored
 28 utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive security measures to protect

1 the confidentiality of user information; (3) Dropbox did not access user data; and (4) all data
2 transmitted via Dropbox was encrypted to ensure secure access.

3 100. Defendant's conduct alleged herein violates the Consumers Legal Remedies Act,
4 including but not limited to, the following provisions: (1) using deceptive representations in
5 connection with goods or services in violation of California Civil Code § 1770(a)(4); (2)
6 representing that goods or services have sponsorship, approval, characteristics, uses, benefits, or
7 quantities which they do not have in violation of Cal. Civ. Code § 1770(a)(5); and/or (3)
8 advertising goods or services with intent not to sell them as advertised in violation of Cal. Civ.
9 Code § 1770(a)(9). As a direct and proximate result of Defendant's conduct, as set forth herein,
10 Defendant has received ill-gotten gains and/or profits including, but not limited to, money.
11 Therefore, Defendant has been unjustly enriched.

12 101. There is no other adequate remedy at law, and Plaintiff and the Class will suffer
13 irreparable harm unless Defendant's conduct is enjoined.

14 102. Pursuant to California Civil Code §§ 1780(a)(2)-(5) and 1780(d) Plaintiff and
15 members of the Class seek an order for: (1) an injunction against Defendant's illegal conduct as
16 alleged herein; (2) restitution; (3) ancillary relief; and (4) attorneys' fees and costs to the full
17 extent allowed by law.

18 103. On May 19, 2011 counsel for Plaintiff and the Class provided Defendant with
19 written notice that its conduct is in violation of the Consumers Legal Remedies Act. Plaintiff and
20 the Class will amend their Complaint after thirty (30) days of having provided this notice to seek
21 damages under the Consumer Legal Remedies Act. *See* Cal. Civ. Code § 1782(d).

22 **FOURTH CAUSE OF ACTION**

23 **VIOLATION OF CALIFORNIA'S FALSE ADVERTISING LAW**

24 **(Cal. Bus. & Prof. Code §§ 17500, *et seq.*)**

25 104. Plaintiff and the Class incorporate by reference the allegations of the preceding
26 paragraphs of this Complaint as if set forth in full herein.

27 105. Dropbox has engaged in false advertising as it disseminated false and/or misleading
28 statements regarding Dropbox.

106. Dropbox knew or should have known by exercising reasonable care that its representations were false and/or misleading. During the Class Period, Dropbox engaged in false advertising in violation of Cal. Bus. & Prof. Code §§ 17500, *et seq.*, by misrepresenting in its advertising, marketing, and other communications disseminated to Plaintiff, the Class, and the consuming public that *inter alia*: (1) third parties including Defendant's employees would not have access to data stored utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive security measures to protect the confidentiality of user information; (3) Dropbox did not access user data; and (4) all data transmitted via Dropbox was encrypted to ensure secure access.

107. Each of these aforementioned representations were false and misleading because during the class period, Dropbox: (1) failed to take adequate steps to secure and encrypt data to prevent access by third parties including Defendant's employees and agents; (2) failed to employ the industry best security measures utilized by its competitors; (3) accessed user information without consent; and (4) failed to ensure that the data transmitted via mobile devices occurred over an encrypted channel.

108. By disseminating and publishing these statements in connection with the sale of Dropbox, Defendant has engaged in and continues to engage in false advertising in violation of Bus. & Prof. Code §§ 17500, *et seq.*

109. As a direct and proximate result of Dropbox's conduct, as set forth herein, Dropbox has received ill-gotten gains and/or profits, including, but not limited to money. Therefore, Dropbox has been unjustly enriched. Pursuant to Cal. Bus. & Prof. Code § 17535, Plaintiff requests restitution and restitutionary disgorgement for all sums obtained in violation of Cal. Bus. & Prof. Code §§ 17500, *et seq.*

110. Plaintiff seeks injunctive relief, restitution, and restitutionary disgorgement of Dropbox's ill-gotten gains as specifically provided in Cal. Bus. & Prof. Code § 17535.

111. Plaintiff and the Class seek to enjoin Defendant from engaging in these wrongful practices, as alleged herein, in the future. There is no adequate remedy at law and if an injunction is not ordered, Plaintiff and the Class will suffer irreparable harm and/or injury.

///

FIFTH CAUSE OF ACTION**VIOLATION OF CALIFORNIA'S UNFAIR COMPETITION LAW****(Cal. Bus. & Prof. Code §§ 17200, *et seq.*)**

112. Plaintiff and the Class incorporate by reference the allegations of the preceding paragraphs of this Complaint as if set forth in full herein.

113. As used in this section, "unfair competition" encompasses three distinct types of misconduct: (a) "any unlawful . . . business act or practice;" (b) "any . . . unfair or fraudulent business act or practice;" and (c) "any . . . unfair, deceptive, untrue or misleading advertising."

114. Dropbox knew or should have known by exercising reasonable care that its representations were false and/or misleading. During the Class Period, Dropbox engaged in false advertising in violation of Cal. Bus. & Prof. Code §§ 17500, *et seq.*, by misrepresenting in its advertising, marketing, and other communications disseminated to Plaintiff, the Class, and the consuming public that *inter alia*: (1) third parties including Defendant's employees would not have access to data stored utilizing Dropbox; (2) Dropbox utilized the industry's most restrictive security measures to protect the confidentiality of user information; (3) Dropbox did not access user data; and (4) all data transmitted via Dropbox was encrypted to ensure secure access.

115. Each of these aforementioned representations were false and misleading because during the class period, Dropbox: (1) failed to take adequate steps to secure and encrypt data to prevent access by third parties including Defendant's employees and agents; (2) failed to employ the industry best security measures utilized by its competitors; (3) accessed user information without consent; and (4) failed to ensure that the data transmitted via mobile phone devices occurred over an encrypted channel.

116. Dropbox's above-described conduct constitutes "unfair" business practices within the meaning of the Unfair Competition Law insofar as Dropbox's business practices alleged herein are immoral, unethical, oppressive, unscrupulous, and/or substantially injurious to consumers.

117. Dropbox's above-described conduct constitutes "fraudulent" business practices within the meaning of the Unfair Competition Law insofar as Dropbox's business practices alleged herein are likely to deceive members of the public.

1 118. These above-described unfair and fraudulent business practices and false and
2 misleading advertising by Dropbox present an ongoing threat to Plaintiff and the Class. Plaintiff
3 is informed and believes, and thereon alleges that Dropbox has systematically perpetrated
4 deceptive and unfair practices upon members of the public and has intentionally deceived Plaintiff
5 and the Class.

6 119. In addition, the use of media to promote the sale of Dropbox through false and
7 deceptive representations constitutes unfair competition and unfair, deceptive, untrue, or
8 misleading advertising within the meaning of the Unfair Competition Law.

9 120. Dropbox further violated the Unfair Competition Law by engaging in unlawful
10 conduct, including but not limited to, failing to comply with Consumers Legal Remedies Act.

11 121. As a direct and proximate result of Dropbox's violation of the Unfair Competition
12 Law, Plaintiff and the Class Members have suffered harm in that they would not have purchased
13 or would have paid less for their Dropbox Pro subscription if Plaintiff and the Class had known
14 that it was not as represented.

15 122. As a direct and proximate result of Defendant's violation of the Unfair Competition
16 Law, Plaintiff and the Class Members have suffered harm in that they reasonably relied on
17 Defendant's misrepresentations and were induced to purchase Dropbox Pro subscriptions.

18 123. As a direct and proximate result of Dropbox's violation of Cal. Bus. & Prof. Code
19 §§ 17200, *et seq.*, Dropbox has been unjustly enriched at the expense of Plaintiff and the Class and
20 should be required to make restitution to Plaintiff and the Class Members or make restitutionary
21 disgorgement of its ill-gotten profits pursuant to Cal. Bus. & Prof. Code § 17203.

22 124. Plaintiff, on behalf of himself and all others similarly situated, demands judgment
23 against Dropbox for injunctive relief and/or restitutionary disgorgement, and an award of
24 attorneys' fees.

25 125. Plaintiff and the Class seek to enjoin Dropbox from engaging in these wrongful
26 practices as alleged herein, in the future. There is no other adequate remedy at law and if an
27 injunction is not ordered, Plaintiff and the Class will suffer irreparable harm and/or injury.
28

PRAYER FOR RELIEF

WHEREFORE, Plaintiff on behalf of himself and all other similarly situated, prays for relief and judgment against Defendant, and each of them, as follows:

1. For an order certifying the Class, and appointing Plaintiff and his counsel to represent the Class;
2. For damages suffered by Plaintiff and the Class;
3. For restitution to Plaintiff and the Class of all monies wrongfully obtained by the Defendant;
4. For preliminary and injunctive relief requiring Defendant to accurately represent the qualities of its services and/or conform its services to its representations;
5. For reasonable attorneys' fees as permitted under applicable statutes;
6. For Plaintiff's costs incurred;
7. For prejudgment interest; and
8. For such other and further relief which the court deems just and proper.

///

///

///

///

///

///

///

///

///

///

///

///

///

///

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiff Joshua Kairoff, on behalf of himself and all others similarly situated, demands a trial by jury of any and all issues in this action so triable.

DATED: May 23, 2011

By: 

DANIEL L. WARSHAW

CLIFFORD H. PEARSON (Bar No. 108523)

cpearson@pswplaw.com

DANIEL L. WARSHAW (Bar No. 185365)

dwarshaw@pswplaw.com

BOBBY POUYA (Bar No. 245527)

bpouya@pswplaw.com

PEARSON, SIMON, WARSHAW & PENNY, LLP

15165 Ventura Boulevard, Suite 400

Sherman Oaks, California 91403

Telephone: (818) 788-8300

Facsimile: (818) 788-8104

JAMES J. PIZZIRUSSO*

jpizzirusso@hausfeldllp.com

HAUSFELD LLP

1700 K Street NW, Suite 650

Washington, DC 20006

Telephone: (202) 540-7200

Facsimile: (202) 540-7201

BRUCE L. SIMON (Bar No. 96241)

bsimon@pswplaw.com

PEARSON, SIMON, WARSHAW & PENNY, LLP

44 Montgomery Street, Suite 2450

San Francisco, California 94104

Telephone: (415) 433 9000

Facsimile: (415) 433 9008

MICHAEL P. LEHMANN (Bar No. 77152)

mlehmann@hausfeldllp.com

HAUSFELD LLP

44 Montgomery Street, Suite 3400

Telephone: (415) 633-1908

Facsimile: (415) 693-0770

Attorneys for Plaintiff Joshua Kairoff and All Others
Similarly Situated

*Admission to practice *pro hac vice* to be submitted

PEARSON, SIMON, WARSHAW & PENNY, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403

AFFIDAVIT OF DANIEL L. WARSHAW PURSUANT TO
CALIFORNIA CIVIL CODE § 1780(d)

Daniel L. Warshaw declares:


1. I am an attorney duly admitted to practice before this Court. I am a partner in the firm of Pearson, Simon, Warshaw & Penny, LLP, attorneys of record for Plaintiff Joshua Kairoff.

2. This action has been filed in a county described in California Civil Code § 1780 as a proper place for the commencement of this action.

3. Defendant Dropbox, Inc. resides in and does substantial business in the San Francisco County, California; a substantial portion of the events complained of by Plaintiff occurred in San Francisco County, California; and the parties have entered into a choice of law provision which requires that Plaintiff file his claim in a court of competent jurisdiction in San Francisco County, California.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 23, 2011, at Sherman Oaks, California.


Daniel L. Warshaw

PEARSON, SIMON, WARSHAW & PENNY, LLP
15165 VENTURA BOULEVARD, SUITE 400
SHERMAN OAKS, CALIFORNIA 91403